



healthplex.

PO Box 8014 Garden City, NY 11530

T 800.468.0608

F 516.745.0079

E accounting@healthplex.com

W healthplex.com

April 14, 2022

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Submitted Via Email:
ldtheft@oag.state.md.us

RE: Privacy Breach Notification
Healthplex File #: 411658

Dear Sir/Madam:

Healthplex is writing to inform you of a recent data incident that affected 52 Maryland residents. On November 24, 2021, we learned that one of our employees fell victim to a phishing attack. Upon learning of the event, Healthplex engaged its privacy office and security incident response teams to investigate the matter. The email account was immediately isolated and the attack was terminated through a reset of the account credentials.

Following a forensic review of the system logging available, we were unable to determine whether or not the threat actor viewed or accessed the data in the impacted email account.

Healthplex engaged a third-party eDiscovery firm to review the contents of the compromised email account. On February 18, 2022, an initial file was returned by the eDiscovery firm and the file was run through our eligibility database to identify impacted individuals. Due to the complexity and at times incompleteness of the data, the eligibility and IT teams had to run the data through multiple iterations of queries.

On April 5, 2022, we confirmed that 52 Maryland residents were impacted as a result of the incident. The information involved may have included the individuals' first and last name, address, group name and number, member ID number, plan affiliation, date of birth, date of service, provider name, ADA codes and their description, billed/paid amounts, prescription drug names, Social Security number, banking information, credit card number, username and password for the member portal, email address, phone number, and driver's license number.

On or about April 15, 2022 written notice will be provided 52 Maryland residents who were affected by this incident. A copy of the template notice letter that will be sent to affected individuals is enclosed.





healthplex.

PO Box 8014 Garden City, NY 11530

T 800.468.0608

F 516.745.0079

E accounting@healthplex.com

W healthplex.com

We will notify other regulatory agencies as required.

We take such matters as this very seriously. There is no evidence to suggest that any affected individuals' information has been misused in anyway. However, as a precaution to help affected individuals monitor the security of their personal information and detect possible misuse of personal information, we are providing a two-year membership in LifeLock identity theft protection program at no cost to the affected individuals. We have also established a dedicated toll-free number for members of the affected population to call, if they have any questions. Additionally, the notification letter sent to affected individuals recommends steps they can take to protect their identity, including informing them that they should report suspected incidents of identity theft to local law enforcement or the attorney general. It also explains to them how to place a fraud alert and/or security freeze on their credit file and provides them with the contact information for the national credit reporting agencies and the Federal Trade Commission.

Protecting the personal information of individuals is very important to us. We maintain an information security program and put additional protections in place to prevent such incidents from occurring in the future, including retraining staff, reinforcing our existing policies and practices, and evaluating additional safeguards.

If you have any questions about this incident, please contact me directly.

Sincerely,

Arthur Cook

Arthur Cook
Associate General Counsel
Healthplex, Inc.
P: 516-419-1764 | E: ArthurC@Healthplex.com





[Date]

[Name]

[Address Line 1]

[Address Line 2]

[City, STATE, Zip Code]

Dear [Name]

We are writing to inform you of a recent security incident at Healthplex that may have involved some of your personal information. Healthplex discovered that an employee was the victim of a phishing attack resulting in unauthorized access to their email account on November 24, 2021.

Healthplex immediately took steps to secure its environment and begin an investigation. The investigation included determining what happened and whether any protected personal information may have been accessed or acquired without authorization.

After completing a comprehensive review of the data potentially affected by the unauthorized access, we determined on April 5, 2022, that your personal information may have been impacted by this incident.

The information that may be involved includes your first and last name, address, group name and number, member ID number, plan affiliation, date of birth date of service, provider name, ADA codes and their description, billed/paid amounts, prescription drug names, Social Security number, banking information, credit card number, username and password for the member portal, email address, phone number, and driver's license number.

In addition to taking the steps described above, Healthplex also implemented additional safeguards to ensure the security of its environment and to reduce the risk of a similar incident occurring in the future, including the implementation of multifactor authentication for all email accounts.

While we have no indication your information was misused, as a precaution we recommend that you regularly monitor the explanation of benefits statements that you receive from us, as well as your bank and credit card statements and tax returns to check for any unfamiliar activity. If you notice any health care services that you did not receive listed on an explanation of benefits statement, please contact us at the number on the back of your ID card. If you do not regularly receive explanation of benefits statements, you may request that we send you these statements following the provision of any health care services in your name or plan number by contacting us at the number on the back of your ID card. If you notice any suspicious activity on either your bank or credit card statement, or tax returns, please immediately contact your financial institution and/or credit card company, or relevant institution.

Additionally, we are offering you free "LifeLock® Identity Theft Protection Services," which proactively protects your personal and financial information and provides comprehensive recovery services if you become a victim of identity theft during your LifeLock membership.





healthplex.

333 Earle Ovington Blvd, Suite 300, Uniondale, NY 11553

T 800.468.0608
F 516.794.3186
E info@healthplex.com
W healthplex.com

Details of your complimentary membership are enclosed along with instructions for registering for this service. The enclosed Reference Guide provides additional steps you may take to monitor and protect your credit and finances.

Furthermore, we established a dedicated toll-free hotline you can call if you have any questions about this notice. You may reach us Monday – Friday between 8:00am and 6:00pm EDT. The toll-free telephone number is 866-540-5917.

Healthplex takes this matter very seriously and is committed to protecting the privacy and security of your personal information. We are reinforcing our existing policies and practices with employees and will continue to evaluate additional safeguards to help prevent a similar incident from occurring in the future. We deeply regret any inconvenience or concern caused by this incident.

Sincerely,

Jackie Cutshall, CIPP/US, FLMI
Privacy Manager/Sr. Investigator





healthplex.

333 Earle Ovington Blvd, Suite 300, Uniondale, NY 11553

T 800.468.0608
F 516.794.3186
E info@healthplex.com
W healthplex.com



NortonLifeLock Identity Theft Protection Services

Healthplex has partnered with NortonLifeLock, an industry leader in identity theft protection, to offer you two years of LifeLock service at no cost to you. Your promotional code is only valid for you and no one else.

Details on Your Complimentary LifeLock Identity Theft Protection Are Below.

You can enroll in LifeLock service by **phone** or **online**. You have until **June 15, 2022** to sign up for your membership.

Enroll by Telephone:

1. Call LifeLock at **1-800-899-0180**. LifeLock representatives are available 24 hours a day, 7 days a week, 365 days a year.
2. Give the LifeLock representative your promotional code: **XXXXXX**
3. Give the LifeLock representative your LifeLock Member ID. Your LifeLock Member ID is your first and last name with no spaces (Ex. Anthony Smith would be anthonymsmith).

Enroll Online:

1. Go to www.LifeLock.com.
2. Click on the **Start Membership** box in the middle of the webpage.
3. You will be taken to another page where, below the FOUR protection plan boxes, you will see the **Promo Code** box. Enter the **Promo Code: XXXXXX** and click the **Apply** button.
4. Enter your first and last name (no spaces) in the LifeLock **Member ID** box (Ex. Anthony Smith would be anthonymsmith) and click **Apply**.
5. Your complimentary offer is presented. Click the red **"START YOUR MEMBERSHIP"** button.

You will receive a welcome email or letter from LifeLock confirming your enrollment has been processed, although your protection begins immediately.

If you have questions about the services offered or enrollment in LifeLock identity theft protection, please call **1-800-899-0180**.





healthplex.

333 Earle Ovington Blvd, Suite 300, Uniondale, NY 11553

T 800.468.0608
F 516.794.3186
E info@healthplex.com
W healthplex.com



Once you have completed the LifeLock enrollment process, the service will be in effect. Your **LifeLock Standard™** membership includes:

- ✓ LifeLock Identity Alert™ System†
- ✓ 24/7 Live Member Support
- ✓ Dark Web Monitoring**
- ✓ LifeLock Privacy Monitor™
- ✓ Lost Wallet Protection
- ✓ Stolen Funds Reimbursement up to \$25,000 †††
- ✓ Personal Expense Compensation up to \$25,000 †††
- ✓ Coverage for Lawyers and Experts up to \$1 million †††
- ✓ U.S.-Based Identity Restoration Team
- ✓ One-Bureau Credit Monitoring^{1**}
- ✓ Reduced Pre-Approved Credit Card Offers
- ✓ USPS Address Change Verification

¹ If your plan includes credit reports, scores, and/or credit monitoring features ("Credit Features"), two requirements must be met to receive said features: (i) your identity must be successfully verified with Equifax; and (ii) Equifax must be able to locate your credit file and it must contain sufficient credit history information. IF EITHER OF THE FOREGOING REQUIREMENTS ARE NOT MET YOU WILL NOT RECEIVE CREDIT FEATURES FROM ANY BUREAU. If your plan also includes Credit Features from Experian and/or TransUnion, the above verification process must also be successfully completed with Experian and/or TransUnion, as applicable. If verification is successfully completed with Equifax, but not with Experian and/or TransUnion, as applicable, you will not receive Credit Features from such bureau(s) until the verification process is successfully completed and until then you will only receive Credit Features from Equifax. Any credit monitoring from Experian and TransUnion will take several days to begin after your successful plan enrollment.

No one can prevent all identity theft or cybercrime. † LifeLock does not monitor all transactions at all businesses.

** These features are not enabled upon enrollment. Member must take action to get their protection.

††† Reimbursement and Expense Compensation, each with limits of up to \$25,000 for Standard. And up to \$1 million for coverage for lawyers and experts if needed. Benefits under the Master Policy are issued and covered by United Specialty Insurance Company (State National Insurance Company, Inc. for NY State members). Policy terms, conditions and exclusions at: LifeLock.com/legal.





Reference Guide

Order Your Free Credit Report

You are entitled to receive your credit report from each of the three national credit reporting agencies once per year, free of charge. You may obtain your free annual credit report from each of the national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free at 1-877-322-8228, or by mailing your request to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually. They provide free annual credit reports only through the website or toll-free number.

When you receive your credit report(s), review them carefully. Look for any inaccurate information and contact the appropriate credit reporting agency to notify of any incorrect information, including accounts you did not open; requests for your credit report from anyone that you did not apply for credit with; or inaccuracies regarding your personal identifying information, such as your home address and Social Security number. If you find anything that you do not understand or that is incorrect, contact the appropriate credit reporting agency using the contact information on the credit report as soon as possible so the information can be investigated, and if found to be in error, corrected.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in your financial accounts, promptly notify your credit card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission. If you believe your identity has been stolen, the U.S. Federal Trade Commission ("FTC") has created a one-stop resource site that provides an interactive checklist that walks through the steps people need to take upon learning that their identity has been stolen or their personal information has been compromised in a data breach. The FTC recommends that you take these additional 4 steps right away when you become a victim:

Step 1: Call the companies where you know fraud occurred.

Step 2: Place a fraud alert and get your credit report.

Step 3: Report identity theft to the FTC.

Step 4: File a report with your local police department.

A checklist of the steps listed above and links to forms and other helpful information can be found on the site at IdentityTheft.gov/steps.

You can learn more about how to protect yourself from becoming a victim of identity theft by contacting the FTC at the address below or visiting the website below:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-438-4338
1-866-653-4261 (TTY)
<http://www.consumer.ftc.gov/features/feature-0014-identity-theft>

Place a Fraud Alert on Your Credit File





To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Credit Agency	Mailing Address	Phone Number	Website
Equifax	Equifax Information Services LLC P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Fraud Request Form *Mail the fraud request form to the address listed above.	1-800-525-6285	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
Experian	Experian P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	https://fraud.transunion.com/

Place a Security Freeze on Your Credit File

You may wish to place a “security freeze” on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. The credit bureaus may charge a reasonable fee to place a freeze on your account and may require that you provide proper identification prior to honoring your request. You can request a security freeze by contacting the credit bureaus at:

Credit Agency	Mailing Address*	Phone Number	Website
Equifax	Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	Automated line: 1-800-349-9960 Customer Care: 1-888-298-0045	https://www.equifax.com/personal/credit-report-services/credit-freeze/





	Equifax Freeze Request Form *Mail the freeze request form to the address listed above.		
Experian	Experian P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com/freeze
TransUnion	TransUnion P.O. Box 160 Woodlyn, PA 19016	1-888-909-8872	https://www.transunion.com/credit-freeze

Additional Attorney General Office Identity Theft Resources. You can obtain information from your state's Attorney General's Office about steps that you can take to help prevent identify theft. Please see the information below for states that provide these resources:

For California Residents. You can obtain additional information from the California Department of Justice's Privacy Enforcement and Protection Unit (<https://oag.ca.gov/privacy>) to learn more about protection against identity theft.

For District of Columbia Residents. You can obtain additional identity theft information from the District of Columbia's Attorney General Office (<https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft>) to learn more about protection against identity theft.

For Maryland Residents. You can contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
25th Floor
Baltimore, MD 21202

Phone: 1-410-576-6491

Fax: 1-410-576-6566

Email: idtheft@oag.state.md.us

Website: <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>

For North Carolina Residents You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001

Phone: 1-877-566-7226 (Toll-free within North Carolina), 1-919-716-6000





Website: <https://ncdoj.gov/>

Identity Theft Link: [Protecting Your Identity - ID Theft Protection by NC DOJ.](#)

For Oregon Residents. You can obtain additional identity theft information from the Oregon Attorney General Office (<https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/>) to learn more about protection against identity theft.

For Rhode Island Residents. You can contact the Rhode Island Attorney General at:

Rhode Island Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903

Phone: 1-401-274-4400

Fax: 1-401-462-9532

Email: DBR.Insurance@dbr.ri.gov

Website: <http://www.riag.ri.gov/ConsumerProtection/About.php#>

Precautions to Help You Avoid Becoming a Victim

1. Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about you, your employees, your colleagues or any other internal information. If an unknown, individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
2. Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
3. Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
4. Do not send sensitive information over the Internet before checking a website's security (for more information, see Protecting Your Privacy, <http://www.us-cert.gov/ncas/tips/ST04-013>).
5. Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
6. If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (<http://www.antiphishing.org>).
7. Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (for more information, see Understanding Firewalls, <http://www.us-cert.gov/ncas/tips/ST04-004>; Understanding Anti-Virus Software, <http://www.us-cert.gov/ncas/tips/ST04-005>; and Reducing Spam, <http://www.us-cert.gov/ncas/tips/ST04-007>).
8. Take advantage of any anti-phishing features offered by your email client and web browser.
9. Employees should take steps to monitor their personally identifiable information and report any suspected instances of identity theft to the FBI's Internet Crime Complaint Center at www.ic3.gov.

